CLAIMS

What is claimed is:

1. A method for detecting viruses in software, comprising:
(a) comparing data with a plurality of virus definitions in a first database;
(b) executing a security event if the data is successfully compared with at least one of the virus definitions;
(c) comparing the data with fingerprints of innocent data in a second database;
(d) allowing access to the data if the data is successfully compared to the fingerprints of innocent data; and
(e) transmitting information to a server for analysis purposes if the data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data.

2. The method as recited in claim 1, wherein the security event is selected from the group consisting of cleaning the data, quarantining the data, and blocking the data.

3. The method as recited in claim 1, and further comprising reporting that the data is innocent if the data is successfully compared to the fingerprints of innocent data.

4. The method as recited in claim 1, wherein the information transmitted to the server includes the data.

5. The method as recited in claim 1, wherein the information transmitted to the server includes a fingerprint associated with the data.

6. The method as recited in claim 5, and further comprising comparing the fingerprint associated with the data and fingerprints associated with innocent data in a third database at the server.

7. The method as recited in claim 6, and further comprising comparing the fingerprint associated with the data and fingerprints associated with virus definitions in a fourth database at the server.

8. The method as recited in claim 7, wherein the third and fourth databases are updated more frequently than the first and second databases.

9. The method as recited in claim 7, and further comprising transmitting the data to the server utilizing the network upon an unsuccessful comparison of the fingerprint associated with the data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database at the server.

10. The method as recited in claim 9, and further comprising analyzing the data transmitted to the server.

11. The method as recited in claim 9, wherein the data is transmitted to the server in separate parts.

12. The method as recited in claim 10, and further comprising updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis.

13. The method as recited in claim 1, wherein the information is transmitted to the server via the Internet.

14. The method as recited in claim 1, wherein the first database and the second database are both components of a client computer coupled to the server via the network.

15. A computer program product for detecting viruses in software, comprising:
(a) computer code for comparing data with a plurality of virus definitions in a first database;
(b) computer code for executing a security event if the data is successfully compared with at least one of the virus definitions;
(c) computer code for comparing the data with fingerprints of innocent data in a second database;
(d) computer code for allowing access to the data if the data is successfully compared to the fingerprints of innocent data; and
(e) computer code for transmitting information to a server for analysis purposes if the data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data.

16. The computer program product as recited in claim 15, wherein the security event is selected from the group consisting of cleaning the data, quarantining the data, and blocking the data.

17. The computer program product as recited in claim 15, and further comprising computer code for reporting that the data is innocent if the data is successfully compared to the fingerprints of innocent data.

18. The computer program product as recited in claim 15, wherein the information transmitted to the server includes the data.

19. The computer program product as recited in claim 15, wherein the information transmitted to the server includes a fingerprint associated with the data.

20. The computer program product as recited in claim 19, and further comprising computer code for comparing the fingerprint associated with the data and fingerprints associated with innocent data in a third database at the server.

21. The computer program product as recited in claim 20, and further comprising computer code for comparing the fingerprint associated with the data and fingerprints associated with virus definitions in a fourth database at the server.

22. The computer program product as recited in claim 21, wherein the third and fourth databases are updated more frequently than the first and second databases.

23. The computer program product as recited in claim 21, and further comprising computer code for transmitting the data to the server utilizing the network upon an unsuccessful comparison of the fingerprint associated with the data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database at the server.

24. The computer program product as recited in claim 23, and further comprising computer code for analyzing the data transmitted to the server.

25. The computer program product as recited in claim 24, wherein the data is transmitted to the server in separate parts.

26. The computer program product as recited in claim 24, and further comprising computer code for updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis.

27. The computer program product as recited in claim 15, wherein the information is transmitted to the server via the Internet.

28. The computer program product as recited in claim 15, wherein the first database and the second database are both components of a client computer coupled to the server via the network.

29. A system for detecting viruses in software, comprising:

(a) logic for comparing data with a plurality of virus definitions in a first database;

(b) logic for executing a security event if the data is successfully compared with at least one of the virus definitions;

(c) logic for comparing the data with fingerprints of innocent data in a second database;

(d) logic for allowing access to the data if the data is successfully compared to the fingerprints of innocent data; and

(e) logic for transmitting information for analysis purposes if the data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data.

30. A client-based method for detecting viruses in software, comprising:

(a) comparing data with a plurality of virus definitions in a first database;

(b) executing a security event if the data is successfully compared with at least one of the virus definitions;

(c) comparing the data with fingerprints of innocent data in a second database;

(d) reporting that the data is innocent if the data is successfully compared to the fingerprints of innocent data; and

(e) transmitting the data over a network for analysis purposes if the data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data.

31. A server-based method for detecting viruses in software, comprising:
(a) receiving a fingerprint associated with data from a client computer for analysis purposes upon the data being unsuccessfully compared to virus definitions and fingerprints of innocent data stored on the client computer;
(b) comparing the fingerprint associated with the data and fingerprints associated with fingerprints of innocent data at a server;
(c) comparing the fingerprint associated with the data and fingerprints associated with virus definitions at the server;
(d) requesting the data from the client computer utilizing the network upon an unsuccessful comparison of the fingerprint associated with the data, and the fingerprints associated with the innocent data and the virus definitions at the server;
(e) receiving the data transmitted from the client computer in response to the request;
(f) analyzing the data transmitted from the client computer; and
(g) updating at least one of the virus definitions and the fingerprints of innocent data based on the analysis.

32. A server-based method for detecting viruses in software, comprising:
(a) receiving a fingerprint associated with data from a client computer for analysis purposes upon the data being unsuccessfully compared to virus definitions stored on the client computer;
(b) comparing the fingerprint associated with the data, and fingerprints associated with virus definitions at a server;
(c) requesting the data from the client computer utilizing the network upon an unsuccessful comparison of the fingerprint associated with the data, and the fingerprints associated with the virus definitions at the server;
(d) receiving the data transmitted from the client computer in response to the request;
(e) analyzing the data transmitted from the client computer; and
(f) updating the virus definitions based on the analysis.

33. A server-based security method, comprising:

(a) receiving a fingerprint associated with data from a client computer for analysis purposes upon the data being unsuccessfully compared to fingerprints associated with innocent data stored on the client computer;

(b) comparing the fingerprint associated with the data, and fingerprints associated with innocent data at a server;

(c) requesting the data from the client computer utilizing the network upon an unsuccessful comparison of the fingerprint associated with the data, and the fingerprints associated with the innocent data at the server;

(d) receiving the data transmitted from the client computer in response to the request;

(e) analyzing the data transmitted from the client computer; and

(f) updating the fingerprints associated with the innocent data based on the analysis.